POLICY 2.00 INTRUSION DETECTION SYSTEMS (IDS)

The Office for Information Resources (OIR) is responsible for, and has the authority to establish and control, intrusion detection configuration and management to protect information technology resources from unauthorized external access attempts.

PURPOSE:

To ensure information technology resources are protected from unauthorized access, modification, destruction or disclosure.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994

OBJECTIVES:

1. To implement proactive enhancements to network security through the early detection of security threats or unauthorized access attempts.
2. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The scope includes any attempt to gain unauthorized access to view, copy, alter, destroy, misconfigure, or redirect any state information resource system, application, service, or data across the State's enterprise.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Identify network locations where IDS will be deployed.
2. Install and manage IDS to ensure the timely detection and blocking of network intrusions and security breaches.
3. Monitor network and system activities for the presence of unauthorized access attempts.
4. Review and maintain reports of suspicious system or network behavior and events, and take appropriate actions.
5. Limit access to specific systems or networks as required.

Agency

1. Implement agency processes and procedures in support of State IDS policy and procedures.

2. Refrain from implementing agency procedures, processes or practices that would expose networked information resources to unnecessary or unauthorized risks.

Individual Users/Clients

1. Adhere to statewide and agency policies, standards, procedures and guidelines with respect to external networks, systems, applications and data security.
2. Refrain from behaviors that would expose networked information technology resources to unnecessary or unauthorized risks.